

Estils



Rebel·lió pel dret a la intimitat

NEREIDA CARRILLO
BARCELONA

L'escuma de la cervesa rellisca fins a la barra pigmentada de molles de pa i volves de cel·lulosa. La noia de l'uni-forme agafa el micròfon: "Harry Potter ja pot venir a buscar els seus entrepans". Mentrestant, en un altre establiment, sona, repetitiva i enèrgica, una música de piano infantil i un osset amb epidermis de cotó i panxa incandescent atreu els compradors amb intermitències. A la caixa, una persona emplena el formulari per obtenir la targeta client. En arribar a la casella de la data de naixement, acostat el bolígraf a la comissura dels llavis, decidint què hi posa, com si pensés a inventar-se la dada.

Escenes com aquestes resulten cada vegada més habituals. Són fruit

Els internautes actuen contra la falta de privacitat mentint sobre les seves dades personals quan les han de facilitar

de la conscienciació ciutadana que cal protegir la privacitat i ser gelosos amb les dades personals que donem. Però els experts hi veuen, també, una actitud d'afartament, de resistència, fins i tot de rebel·lia contra el fet que ens demanin les dades per tot i que s'utilitzin de forma fraudulenta i invasiva. Cada vegada hi ha més ciutadans que desactiven la geolocalització del mòbil, que fan servir l'encriptació com a mode segur per comunicar-se o que menteixen quan han d'omplir un formulari en una botiga.

L'ofuscació és un mètode cada vegada més habitual. Un terme que Gemma Galdon, professora de la Universitat de Barcelona i sòcia fundadora d'Éticas Research & Consulting, una consultoria especi-

Empreses
Uber té més dades de mobilitat a Barcelona que l'Ajuntament

alitzada en seguretat i privacitat, defineix com a "mentir de forma sistemàtica quan dones les teves dades perquè les bases de dades creades pel *big data* no tinguin cap mena de qualitat". Galdon demana que quan donem informació de caràcter personal pensem si és una dada necessària o no i si ens aportarà algun benefici: "Si l'únic que rebem a canvi són uns cèntims de descompte quan comprem el pollastre, potser no cal donar la nostra data de naixement".

Vigilància subvertida

El rebuig a la vigilància constant no és nou. Algunes de les primeres càmeres de videovigilància que es van instal·lar a l'espai públic van acabar destrossades per actes vandàlics. A

Madrid, l'any 2010, els veïns de Lavapiés van empaperar el barri amb missatges crítics amb la càmera instal·lada pel consistori. "Lavapiés, 1984", deien els pòsters, en referència a l'obra de George Orwell. Més enllà del vandalisme i la protesta, l'activisme també ha explorat fórmules per protegir la privacitat. "Hi ha molta gent investigant com subvertir la tecnologia i com mantenir la privacitat en un món de vigilància continuada", explica la professora de la UB. En aquest sentit, l'artista i tecnòleg Adam Harvey ha creat formes de maquillatge, pentinat i roba per enganyar els sistemes de detecció facial i també una col·lecció tèxtil que impedeix ser detectat per drons.

Davant de situacions d'abús, Simona Levi, fundadora del partit Xi i activista per a la democràcia a internet, insta a "no signar sessions de dades massa invasives". Però això



01 i 02. L'artista i tecnòleg Adam Harvey ha creat una col·lecció tèxtil que impedeix ser detectat per drons.
03 i 04. Harvey també ha inventat formes de maquillatge, pentinat i roba per enganyar els sistemes de detecció facial. ADAM HARVEY

no és possible gairebé mai: les aplicacions, les xarxes socials i altres productes d'internet exigeixen a l'usuari les seves dades o li deneugen el servei. “L'escenari que defensem –explica Galdon– és aquell en què tu puguis decidir si dones les dades o no. Això ara mateix no existeix”. Amb aquest horitzó (que l'usuari tingui el control sobre les seves dades) treballen en el projecte Decode l'Ajuntament de Barcelona, investigadors de la UOC i experts d'altres institucions del Regne Unit, Suècia i França.

Dades públiques i incorruptibles
Mayo Fuster, directora del grup de recerca Digital Commons de la UOC i investigadora del projecte, explica que estan treballant, a diferents nivells, per millorar la gestió de la privacitat dels ciutadans. Així, impulsaran maquinari “que no tingui components que permetin l'espionatge”, però també plataformes en què l'usuari sigui més conscient de qui utilitza les seves dades i per què i que pugui aturar usos inadequats. El projecte, amb un finançament europeu de cinc milions d'euros, fa servir

tecnologia *blockchain*. “Tothom qui hi participa té accés a les dades en les mateixes condicions i ningú pot corrompre-les. Perquè hi hagi un determinat ús de les dades, tothom ho ha de validar”, explica Fuster.

Aquesta situació de transparència i de poder de l'usuari està lluny de la situació actual. Els gegants tecnològics abusen de la informació personal. Ho ha provat recentment ProPublica, una agència i pàgina web de periodisme d'investigació guardonada amb el premi Pulitzer. Segons una investigació seva, Facebook compra informació a *brokers* de dades sobre la vida *offline* dels seus usuaris per creuar-la amb les seves pròpies dades. Levi assegura que tothom que està a Facebook està “hipervigilat” i aplau-deix que els adolescents emprin alternatives com ara Snapchat o Telegram. El recel a aquest gegant tecnològic ve de lluny. Així, el 2009, l'artista Owen Mundy va crear l'eina Give Me My Data per exportar les dades de Facebook. Es van popularitzar eines similars com la Suicide Machine o l'Account Killer, per esborrar els comptes de xarxes socials.

Drets i lliure competència

Entre el tot o res, cal trobar solucions intermèdies a favor de la privacitat. Fuster explica que Decode té aquesta intenció. Afegeix que s'aplicarà sobretot a l'economia col·laborativa i a processos de participació. La idea és resoldre problemes actuals de privacitat, però també evitar la privatització del coneixement. “En aquests moments –lament Fuster–, Uber té més dades de mobilitat a Barcelona que l'Ajuntament. Per això, té una situació de privilegi respecte a l'administració i respecte als competidors”. Per a la investigadora de la UOC, ara mateix tant els usuaris com l'administració i les altres empreses estan en una situació vulnerable. L'individu, perquè desconeix si s'estan vulnerant els seus drets; l'administració, perquè “no pot tenir accés a dades que són molt rellevants per a la gestió pública i no pot vetllar pel compliment dels drets dels ciutadans”, i les empreses, perquè “es creen conglomerats de dades que no permeten la lliure competència”.

“Les dades personals –opina Levi– han d'estar molt protegides; però les dades massives haurien de ser accessibles i no només propietat de les empreses o els ajuntaments sinó de tots els ciutadans”. Les expertes consultades advoquen per empoderar l'usuari, no només perquè controli les dades que tenen d'ell els gegants tecnològics sinó també perquè pugui decidir sobre la tecnologia. “La indústria actual crea mecanismes de *dessobirania*”, es queixa Fuster. I adverteix: “La tecnologia està tan articulada en tots els àmbits de la societat que difícilment tindrem sobirania en qualsevol àmbit si no tenim sobirania tecnològica”. ■

Consells per recuperar el control sobre les pròpies dades

No deixis rastre

Pots desactivar la geolocalització del teu telèfon mòbil o fer servir fundes de mòbil amb protecció d'ones que eviten que t'agafin dades.

Vigila que no t'escoltin

Cal tapar la webcam i les sortides del so dels dispositius. Les últimes revelacions de Wikileaks van provar que la CIA espiava a través de televisors intel·ligents.

Només wifis segurs

Connectar-se a wifis de restaurants o hotels pot comportar riscos; altres persones poden accedir a les nostres dades.

Busca, però que no et trobin

Hi ha alternatives a Google, com ara els cercadors Duck Duck Go o Startpage, que no compilen ni comparteixen informació dels usuaris.

Encriptar, una bona opció

L'encriptació està guanyant pes com a opció de transmissió segura. Es pot encriptar el correu electrònic o la informació de l'ordinador. El sistema de navegació Tor utilitza connexions encriptades.